Pseudo Random DNS Query Attacks & Resolver Mitigation Approaches
The attacks

- Began in February 2014
- Attack intent is to DDoS DNS authoritative provider, but incidentally degrades ISP resolvers
The parties involved

- Sometimes this is an extortion attack
- Frequently seems to originate and terminate in China

- Target domain may be hosted with many non-targeted domains
- Targets hop from provider to provider

Initiator of DDoS traffic

Target of the DDOS Authoritative provider
Identifying the attack

high volume of queries for non-existent sub-domains

<randomstring>.www.example.com
<anotherstring>.www.example.com

does not exist

exists

??
**Attack begins**

**Insecure Home gateways**
Home users are unaware

1. Requests for randomstring.www.example.com

2. Attempt to resolve

**example.com**
Target of the DDOS Authoritative provider

**Initiator of DDoS traffic**

**ISP resolvers**
nothing about this in the cache

© 2014 ISC
Initially, the target responds

1. The Initiator sends a request (e.g., DNS query) to the Home gateway.

2. The Home gateway forwards the request to the ISP resolvers.

3. The Server replies with "no such domain" to the ISP resolvers.

4. The ISP resolvers reply (NXDOMAIN) to the Home gateway.

Example: example.com

- Insecure Home gateways
- ISP resolvers: Authoritative provider of example.com
- Home users are unaware of the DDoS attack.
More requests flood in

1. More requests for randomstrings.www.example.com

Insecure Home gateways

Home users are unaware

Issuer of DDoS traffic

Example.com

Target of the DDoS Authoritative provider

ISP resolvers
Target is overwhelmed

Insecure Home gateways

Home users are unaware

Initiator of DDoS traffic

ISP resolvers

2. Attempt to resolve

3. Server is unresponsive

example.com

Target of the DDoS Authoritative provider

© 2014 ISC
Resolver is degraded

Insecure Home gateways

Home users are unaware

Initiator of DDoS traffic

ISP resolvers

Waiting for responses

3. Server is unresponsive

dexample.com

Target of the DDoS Authoritative provider

© 2014 ISC
Legitimate queries fail

1. Request for www.example.com

Insecure Home gateways

Home users are unaware

Initiator of DDoS traffic

ISP resolvers

Waiting for responses

Target of the DDoS
Authoritative provider
MITIGATION TECHNIQUES

What can we do?

What has been tried in production?
Stage 1: “hair on fire”
LIE
(about authority)
Create a local answer

- Make recursive server temporarily authoritative for the target domain

- Problem of false-positives (might need white-lists if using scripted detection)
- Manual configuration change
- Need to undo the mitigation afterwards
Stage 2: Consider Automated filtering

(Near) Real Time Block Lists

- Detect ‘bad’ domain names or just the problematic queries & filter them at ingress to the resolver
- Nominum Vantio
- BIND DNS-RPZ
- There are usually fees associated with feeds
Stage 3: Consider making your resolvers smarter

- Monitor responses vs timeouts
- Adjust throttle
- Throttle back queries
- Monitor responses vs timeouts
PER ZONE

PER SERVER
fetches-per-server

- Per-server quota dynamically re-sizes itself based on the ratio of timeouts to successful responses.
- Completely non-responsive server eventually scales down to fetches quota of 2% of configured limit.
- Similar in principle to what NLNetLabs is doing in Unbound.
fetches-per-zone

- Works with unique clients
- Default 0 (no limit enforced)
- Tune larger/smaller depending on normal QPS to avoid impact on popular domains
- In practice, this has been the winner so far for those using BIND
Fetches-per-zone at Jazztel

Spanish triple-play ADSL carrier & ISP
Roberto Rodriguez Navio, Jazztel Networking Engineering
used with permission
Still experimental

- Some controversy about adaptive approach vs blacklists
- Whitelists may be needed
- Per-server/zone settings
  - Configurable override parameters for fetch limits on a per zone or per server basis
- SERVFAIL cache (for client retries)
- Improved reporting & statistics
Options Summary

1) Configure your resolver to LIE answer authoritatively yourself
2) Configure a BLACK LIST of domains under attack possibly subscribe to a feed for this
3) Consider ADAPTIVE LIMITS per server per zone
Ideally, close the open resolvers!!

www.shadowserver.org
Good Luck!!!